UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/977,159	10/11/2001	Glen Alan Jaquette	TUC920010022US1	3879

46917 7590 06/24/2009

KONRAD RAYNES & VICTOR, LLP.
ATTN: IBM37
315 SOUTH BEVERLY DRIVE, SUITE 210
BEVERLY HILLS, CA 90212

EXAMINER	
WINTER, JOHN M	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
06/24/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

krvuspto@ipmatters.com

Office Action Summary	Application No.	Applicant(s)	
	09/977,159	JAQUETTE, GLEN ALAN	
	Examiner	Art Unit	
	JOHN M. WINTER	3685	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 March 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-5,7-16 and 44-75* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 3-5, 7-16 and 44-75* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Acknowledgements

The Applicants amendment filed on March 19, 2009 is hereby acknowledged, Claims 1, 3-5, 7-16 and 44-75 remain pending.

Response to Arguments

1. Applicant's arguments with respect to claims 1-17 and 44 have been considered but are moot in view of the new ground(s) of rejection in view of newly discovered reference Levy et al. (US Patent 5,748,744).

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 1-17 and 44-46 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

3. Based on Supreme Court precedent and recent Federal Circuit decisions, § 101 process must (1) be tied to another statutory class (such as a particular apparatus) or (2) transform underlying subject matter (such as an article or materials) to a different state or thing. If neither of these requirements is met by the claim(s), the method is not a patent eligible process under 35 U.S.C. § 101.

4. Claim 1 and 17 discloses a mere nominal recitation of technology and fails to transform the underlying subject matter to a different state, (Examiner note that there is no post solution activity – or actual result achieved) therefore the claimed method is non-

statutory and rejected under 35 U.S.C. 101 (*Diamond v. Diehr*, 450 U.S. 175, 184 (1981); *Parker v. Flook*, 437 U.S. 584, 588 n.9 (1978); *Gottschalk v. Benson*, 409 U.S. 63, 70 (1972); *Cochrane v. Deener*, 94 U.S. 780, 787-88 (1876)).

5. Claims 2-9 and 11-17, 44-46 are dependant upon claims 1 and 10 respectively and are rejected for at least the same reason.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 3-5, 7-16 and 44-75 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shear et al (US PG Pub 2001/0042043) in view of Smythe et al. (US Patent 5,325,430) and further in view of Levy et al. (US Patent 5,748,744).

7. As per claim 1, 10 and 44 Shear et al teaches a method for accessing data in a read/write storage medium within one of a plurality of storage cartridges mounted into a plurality of interface devices comprising:

providing an association of at least one coding key to the plurality of storage cartridges, wherein the coding key associated with the storage cartridge is used to decode and code data in the storage cartridge; (*see figs 1A, 1B, 1C, paragraphs 0078-0081, 0127-0138, 0183, 0193-0199, 0216-0220).*

8. Shear et al. does not specifically disclose decrypting, by the receiving interface device, the coding key encrypted by the host to use for in the I/O request;
using, by the receiving interface device the decrypted coding key to decode data to read in the storage cartridge including the encrypted coding key in response to the I/O request comprising a read request; and using, by the receiving interface device the decrypted coding key to code data to write to the target storage cartridge including the encrypted associated with the decrypted coding key in response to the I/O request comprising a write request.
Smythe et al. discloses receiving, decrypting, by the receiving interface device, the coding key encrypted by the host to use for in the I/O request; (Column 3, lines 40-62) using, by the receiving interface device the decrypted coding key to decode data to read in the storage cartridge including the encrypted coding key in response to the I/O request comprising a read request; and using, by the receiving interface device the decrypted coding key to code data to write to the target storage cartridge including the encrypted associated with the decrypted coding key in response to the I/O request comprising a write request. (Column 7, lines 53-60 [Examiner notes that the terms "to code data to write in the storage cartridge" etc.. is representative of non-functional descriptive information and it has been held such information will not distinguish a claimed device from the prior art (*In re Gulack*, 217 USPQ 401 (Fed. Cir. 1983), *In re Ngai*, 70 USPQ2d (Fed. Cir. 2004), *In re Lowry*, 32 USPQ2d 1031 (Fed. Cir. 1994); MPEP 2106.01).

9. It would be obvious to one having ordinary skill in the art at the time the invention was made to combine the Shear et al's method with Smythe al.'s teaching in order to create a cryptographically protected data volume.

10. Shear et al. does not specifically disclose encrypting the coding keys and storing the encrypted coding keys in the storage cartridges; receiving, by a receiving interface device comprising one of the interface devices, an Input/Output (I/O) request to a target storage cartridge comprising one of the storage cartridges; mounting, by the receiving interface device, the target storage cartridge in response to the I/O request; reading, by the receiving interface device, the encrypted coding key from the mounted target storage cartridge; transmitting, by the receiving interface device, the read encrypted coding key to a host device" receiving, by the receiving interface device, the coding key encrypted by the host;

Levy et al. discloses encrypting the coding keys and storing the encrypted coding keys in the storage cartridges; (Column 4, lines 6-12, and 53-60) receiving, by a receiving interface device comprising one of the interface devices, an Input/Output (I/O) request to a target storage cartridge comprising one of the storage cartridges;(Column 6, lines 33-36) mounting, by the receiving interface device, the target storage cartridge in response to the I/O request; reading, by the receiving interface device, the encrypted coding key from the mounted target storage cartridge; transmitting, by the receiving interface device, the read encrypted coding key to a host device,(Column 5, Line 54 – "Cipher enable" process) receiving, by the receiving interface device, the coding key encrypted by the host; (Column 6, lines 43-52)

11. It would be obvious to one having ordinary skill in the art at the time the invention was made to combine the Shear/Smythe with Levy et al.'s teaching in order to create a cryptographically protected data volume.

12. Claim 44 is not patentably distinct from claim 1, and is rejected for at least the same reasons.

As per claim 2 and 28, Shear et al teach a method of using the coding key to encode data to write to the storage medium; transmitting the encoded data to the interface device to write to the storage medium in one storage cartridge mounted in the interface device; receiving encoded data from the interface device read from the storage medium; and using the coding key to decrypt the received encoded data (see figs 1A, 1B, 1C, paragraphs 0078-0081, 0127-0138, 0183, 0193-0199, 0216-0220).

As per claim 3 Shear et al teach a method wherein the association of the at least one coding key to the plurality of storage cartridges associates one key with the plurality of storage cartridges, wherein the one key is capable of being used to encode data written to the storage medium and decode data read from the storage medium of the plurality of storage devices (see figs 1A, 1B, 1C, paragraphs 0078-0081, 0127-0138, 0183, 0193-0199, 0216-0220).

As per claim 4 Shear et al teach a method wherein the association of the at least one coding key to the plurality of storage cartridges associates a different key with each

storage cartridge, wherein the key associated with one storage cartridge is used to encode data written to the storage medium and decode data read from the storage medium of the storage cartridge (see figs 1A, 1B, 1C, paragraphs 0078-0081, 0127-0138, 0183, 0193-0199, 0216-0220).

13. As per claim 5, 22, 31, Shear et al teach a method wherein the coding key comprises a seed value that is used to generate an additional key that is used to directly decode and encode the data in the storage medium in the storage cartridge (see figs 1A, 1B, 1C, paragraphs 0078-0081, 0127-0138, 0183, 0193-0199, 0216-0220).

As per claim 6, Shear et al teach a method further comprising: transmitting the encrypted coding key to the interface device, wherein the interface device decrypts the coding key to use to decode and code data stored in the storage medium (see figs 1A, 1B, 1C, paragraphs 0078-0081, 0127-0138, 0183, 0193-0199, 0216-0220).

As per claim 7, Shear et al teach a method wherein encrypting the coding key further comprises: encrypting by the host the coding key with a first key, wherein a second key used by the interface device is capable of decrypting the coding key encrypted with the first key (see figs 1A, 1B, 1C, paragraphs 0078-0081, 0127-0138, 0183, 0193-0199, 0216-0220).

As per claim 8, Shear et al teach a method wherein encrypting the coding key further comprises: encrypting the coding key with a first key, wherein a second key is capable

of decrypting the coding key encrypted with the first key; encrypting the second key with a third key, wherein the interface device is capable of decrypting data encrypted with the third key; and transmitting the coding key encrypted with the first key and the second key encrypted with the third key to the interface device (see figs 1A, 1B, 1C, paragraphs 0078-0081, 0127-0138, 0183, 0193-0199, 0216-0220).

As per claim 9, Shear et al teach a method wherein encrypting the coding key further comprises: encrypting the coding key with a first key, wherein a second key is capable of decrypting the coding key encrypted with the first key; transmitting the coding key encrypted with the first key to the interface device; receiving, from the interface device, the coding key encrypted with the first key; decrypting the coding key with the second key; encrypting the coding key with a third key, wherein a fourth key used by the interface device is capable of decrypting data encrypted with the third key; and transmitting the coding key encrypted with the third key to the interface device (see figs 1A, 1B, 1C, paragraphs 0078-0081, 0127-0138, 0183, 0193-0199, 0216-0220).

As per claim 10, Shear et al teach a method for accessing data in a removable storage cartridge including a storage medium, comprising: receiving an encrypted coding key from a host system; decrypting the encrypted coding key; using the coding key to encode data to write to the storage medium; and using the coding key to decode data written to the storage (see figs 1A, 1B, 1C, paragraphs 0078-0081, 0127-0138, 0183, 0193-0199, 0216-0220).

As per claim 11, Shear et al teach a method wherein encoding the data with the coding key compresses the data and wherein decoding the data written to the storage medium decompresses the data, and wherein the data can only be encoded or decoded using the coding key (see figs 1A, 1B, 1C, paragraphs 0078-0081, 0127-0138, 0183, 0193-0199, 0216-0220).

As per claim 12, Shear et al teach a method wherein the coding key is encrypted by a first key maintained at the host system, further comprising; maintaining a second key that is capable of decrypting data encrypted using the first key, wherein the second key is used to decrypt the coding key encrypted with the first key (see figs 1A, 1B, 1C, paragraphs 0078-0081, 0127-0138, 0183, 0193-0199, 0216-0220).

As per claim 13, Shear et al teach a method wherein the second key is stored in an integrated circuit non-volatile memory that is only accessible to decrypting logic that uses the second key to decrypt data encrypted using the first key (see figs 1A, 1B, 1C, paragraphs 0078-0081, 0127-0138, 0183, 0193-0199, 0216-0220).

As per claim 14, Shear et al teach a method further comprising transmitting the coding key decrypted using the decrypting logic to encoder/decoder logic, wherein the encoder/decoder logic uses the coding key to encode and decode data to the storage

medium (see figs 1A, 1B, 1C, paragraphs 0078-0081, 0127-0138, 0183, 0193-0199, 0216-0220).

As per claim 15, Shear et al teach a method comprising: storing the coding key encrypted with the first key within the storage cartridge; receiving an input/output (I/O) request directed to the storage cartridge; and accessing the encrypted coding key from the storage cartridge, wherein the accessed coding key is decrypted using the second key, and wherein the decrypted coding key is used to encode and decode data to execute the I/O request to the storage cartridge (see figs 1A, 1B, 1C, paragraphs 0078-0081, 0127-0138, 0183, 0193-0199, 0216-0220).

As per claim 16, Shear et al teach a method wherein the received encrypted coding key is encrypted by a first key maintained at the host system, wherein the host system maintains a second key that is capable of decrypting data encrypted using the first key, further comprising: receiving, from the host system, the second key encrypted by the host system using a third key, wherein data encrypted using the third key is capable of being decrypted using a fourth key; accessing the fourth key; using the fourth key to decrypt the encrypted second key received from the host system; and using the decrypted second key to decrypt the received coding key encrypted using the first key (see figs 1A, 1B, 1C, paragraphs 0078-0081, 0127-0138, 0183, 0193-0199, 0216-0220).

As per claim 17, Shear et al teach a method wherein the coding key is encrypted by a first key maintained at the host system, wherein the host system maintains a second key that is capable of decrypting data encrypted using the first key, further comprising: transmitting the encrypted coding key received from the host system back to the host system; and in response to transmitting the encrypted coding key back to the host system, receiving, from the host system, the coding key encrypted using a third key, wherein data encrypted using the third key is decrypted using a fourth key; and accessing the fourth key, wherein the coding key is decrypted using the fourth key (see figs 1A, 1B, 1C, paragraphs 0078-0081, 0127-0138, 0183, 0193-0199, 0216-0220). Claims 45-75 are in parallel with the above rejected claims and are rejected for at least the same reasons.

Conclusion

14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JOHN M. WINTER whose telephone number is (571)272-6713. The examiner can normally be reached on M-F 8:30-6, 1st Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Calvin Hewitt can be reached on (571) 272-6709. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JMW

/Calvin L Hewitt II/
Supervisory Patent Examiner, Art Unit 3685